

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

2017 JUN 16 PM 1:55

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
GREGTHATCHER46@GMAIL.COM AND
RESULTSNEW1@GMAIL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE, INC.

Case No.

2:17-mj-60

Filed Under Seal

CLERK

BY LAW
DEPUTY CLERK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jennifer A. Vander Veer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, Inc., an email provider whose Legal Compliance Department is located at 1600 Amphitheatre Parkway, Mountain View, CA 94042 (hereinafter "Google"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Federal Bureau of Investigation (FBI), and have been since 2008. I am assigned to the cyber squad of the FBI's Albany Field Office where I am responsible for investigating high-tech crimes, including cyber-

based terrorism, espionage, computer intrusions, and major cyber fraud. Prior to joining the FBI, I held the position of Internet Operations Manager at a private company in Vermont for eight years, and also worked as a Software Development Intern for a large technology company in California.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(2)(C) (Fraud and related activity in connection with computers) have been committed and that evidence of these violations is stored at premises controlled by Google. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court “is a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. I am aware of the following facts pertinent to the application for a search of information associated with the email addresses listed in Attachment A:

gregthatcher46@gmail.com and resultsnew1@gmail.com.

7. On September 27, 2016, Joseph Finnigan, of the law firm Johnson & Finnigan LLP, South Burlington, Vermont, telephoned the FBI to report that his law firm

had been targeted in an email fraud scheme that resulted in the loss of \$100,683.96 on September 16, 2016.

8. On October 19, 2016, I interviewed Joseph Finnigan who confirmed that his law firm had been defrauded of \$100,683.96. Finnigan stated that his law firm had been representing the buyers in the sale of real estate located at 68 Mountain Road, Westford, Vermont. The closing date was scheduled for September 16, 2016, and the sellers were represented by Wick & Maddocks Law Offices. Johnson & Finnigan LLP paralegal, Hillary Barbour, was handling communications associated with transaction. Finnigan provided copies of Barbour's email communications to and from her work email address, hillary@jflawvt.com, on September 16, 2016, associated with the transaction which I have reviewed:

- a. At 9:47 AM, Barbour received an email from "Liz Hadaway" email address "lizzie.wickandmaddocks@gmx.com." The email stated: "What time are the buyers coming for closing? Thanks, Liz," and included the following email signature "Wick & Maddocks Law Offices, 1 Grove Street, PO Box 8502, Essex, VT 05451-8502, Ph: (802) 872 – 8200, Fax (802) 872-0472." Barbour responded at 9:52 AM and informed "Liz" that that the buyers were coming at 10:00 am and stated that the sellers could arrive at the same time.
- b. At 10:40 AM, lizzie.wickandmaddox@gmx.com replied "Any update as regards the sellers proceeds? The seller want the proceeds wired to their personal trading account, Please advise what information you need to get this done, You can reach me here if you need anything, I will be busy with limited access to my phone.

Thanks, Liz.” The email included the same email signature used in the 9:47 AM email.

- c. At 10:57 AM, Barbour replied, “Hi Liz, This is new to us! They never mentioned it at the closing table and walked away with their check. They would need to bring back the proceeds check and provide us with the wiring information and pay the wiring fee. Thank you, Hillary Barbour.”
- d. At 11:10 AM, lizzie.wickandaddocks@gmx.com replied “Yes, I was shocked as well, I told them they need to bring back the check, but to my surprise, They shredded the check thinking it’s safer. What I will advise is to put a stop on the check before having the proceeds sent, I gave them that option and they are cool with it already. Please and let me know what else you need. Thanks Liz.” The email included the same email signature used in the 9:47 AM email.
- e. At 11:32 AM, Barbour replied “Hi Liz, We need full wiring instructions from their bank and they need to bring in a check for \$60.00 payable to Johnson & Finnigan LLP to pay for the stop payment and the wiring fee. We will not process the wire until we have both of these items in hand. Hillary Barbour.”
- f. At 11:54 AM, lizzie.wickandmaddocks@gmx.com replied “Just reaching out to them and was told how about you deduct the fees from the proceeds, its safer and easier, You can go ahead and deduct the fees from the proceeds, thanks, they need the funds urgently for another closing, so they can’t afford days. Thanks Liz.” The email included the same email signature used in the 9:47 AM email.
- g. At 11:58 AM, Barbour replied, “Okay, will do. Once I have the wiring instructions I will initiate the wire. Thank You, Hillary Barbour.”

- h. At 12:22 PM, lizzie.wickandmaddocks@gmx.com replied "Wiring instructions below." The email included bank account information for a Bank of America account in Houston, Texas, with the account name "Benjamin & Jessica Stuart Thabo, Inc.," and an address in Essex Junction, Vermont. The email concluded "Send the wire receipt when sent. Thanks."
- i. At 12:59 PM, Barbour replied "Hi Liz, Wire has been initiated. The receipt from the bank is attached above! Thank you, Hillary Barbour."
- j. At 1:01 PM, lizzie.wickandmaddocks@gmx.com replied, "Thanks, got it."
- k. At 3:12 PM, lizzie.wickandmaddocks@gmx.com replied, "Do you have any idea if the wire was completed because the funds is yet to hit the sellers account."
- l. At 3:32 PM, Barbour replied, "The wire has gone through. It could be the FED holding it up. But the accounting dept at my bank would have notified me if the funds were bounced back. Thank You, Hillary Barbour."

9. Joseph Finnigan also provided me with a copy of an email received from "Liz" at Wick & Maddocks Law Offices on September 13, 2016, which I have reviewed. This email was from the address lizzie@wickandmaddocks.com, and included the same signature that was attached to the 9:47 AM email on September 16, 2016, described above. Finnigan confirmed that this email address used on September 13, 2016, was the correct address for Wick & Maddocks Law Offices employee Liz Hadaway and that the email address lizzie.wickandmaddocks@gmx.com was not a valid address for Hadaway.

10. Finnigan stated that on September 27, 2016, he was contacted by an attorney at Wick & Maddocks regarding the status of their clients' funds. It was at that point that both attorneys realized that the request to cancel the check and wire the seller's proceeds

was fraudulent. Finnigan was advised by his bank that wired funds could not be recovered because they had already been withdrawn from the receiving account.

11. Finnigan further explained that on September 28, 2016, Hillary Barbour's email account hillary@jflawvt.com was hijacked¹ and she was unable to log in. Barbour's email account was then used by unknown cyber actors to send malicious emails to her contacts that appeared to be about a real estate closing but instead contained a suspicious link to a document.

12. On September 28, 2016, I was contacted by a bank in South Burlington, Vermont, that stated bank employees had received multiple emails from law firms with whom the bank did business. One of the emails which was received on September 28, 2016, was from hillary@jflawvt.com and the subject of the email was "Closing Package." The email stated "Good day, Attached is the fully executed document of the below transaction: To view it, click the document below. confidential.docx. Please take a look and let me know if these are ready to print." The bank advised that the link had appeared to be malicious and that a call to Johnson & Finnigan LLP had confirmed the sending account had been compromised.

13. According to Finnigan, email services for Johnson & Finnigan LLP's business email accounts which utilize the domain name² jflawvt.com, are hosted though

¹ Account hijacking is a process through which an individual's email account, computer account or any other account associated with a computing device or service is stolen by a hacker. Often, the hacker uses the stolen account information to carry out malicious or unauthorized activity by impersonating the account owner.

² A domain name is a registered alphanumeric name with domain suffix such as .com or .net, that is used to identify one or more IP addresses. Domain names are interpreted by computers on the internet through the use of Domain Name System (DNS) servers which translate the domain names into IP addresses. An IP address is a unique string of

Google's Gmail service. Finnigan provided a copy of an email sent on September 29, 2016, from an information technology service provider, Jamie Parent of Transparent Computers, who was contracted by Johnson & Finnigan LLP. The email, which I reviewed, showed that Parent had conducted a review of Barbour's Gmail account following the September 28, 2016, discovery. Parent discovered email rules³ on Hillary's account to camouflage activity, including email forwarding and deletion of key emails. He further explained that "hundreds of Hillary's email have been forwarded to: gregthatcher46@gmail.com."

14. On November 30, 2016, I received Gmail login event records from Google for Barbour's email account hillary@jflawvt.com. I reviewed these records and discovered a number of suspicious login events including the following:

- a. On August 7, 2016, there was an account login from an IP address associated with servers registered to an address in Nigeria.
- b. On August 17, 2016, there was an account login from an IP address associated with servers registered to an address in Nigeria.
- c. On September 14, 2016, there was an account login from an IP address registered to LeaseWeb USA, Inc. On November 11, 2016, I received information from LeaseWeb USA, Inc. showing that the IP address belonged to LeaseWeb USA, Inc. customer ZenGuard GmbH. I conducted a review of open source information

numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

³ According to Google's Gmail Help website, users of Gmail can manage incoming email by using Gmail's filters to label, archive, delete, star, or automatically forward email according to rules set by the account user. Filters can be defined using a variety of criteria, including contents of the From, To, or Subject headers; search terms; and message size.

regarding ZenGuard GmbH and determined that the company is the provider of the VPN service ZenMate⁴.

- d. On September 25, 2016, there was an account login from an IP address associated with servers registered to an address in Malaysia.
- e. On September 28, 2016, there was an account login from an IP address associated with servers registered to an address in Nigeria.

15. On December 12, 2016, Hillary Barbour confirmed in an email to me that she did not have an account with ZenMate. She had only ever accessed her work email from her two work computers and her personal cell phone and iPad. On June 14, 2017, I received verbal confirmation from Hillary Barbour that she had never traveled to Nigeria or Malaysia.

16. On November 15, 2016, the FBI received records from Bank of America, which I have reviewed. These records showed that the Bank of America account that had received the September 16, 2016, wire transfer from Johnson & Finnigan LLP had been closed on October 28, 2016. The account holder name was listed as Neo Nthanda Thabo and the identification utilized to open the account was listed as a "Foreign Passport W/Photo." I was unable to locate any individuals with that name in driver license or passport databases.

17. On February 22, 2017, I received an email from Hillary Barbour stating that she had received an email that day from what appeared to be a fraudulent email account

⁴ ZenMate (zenmate.com) is a virtual private network (VPN) provider that creates a secure and encrypted connection between the user and a ZenMate server on the internet. The service allow users to appear to have an IP address in 30 or more countries, including the United States. ZenMate advertises that it does not keep logs, so the connection activity of its customers is not retained. A cyber actor could utilize a service like ZenMate to help conceal his/her true location and identity.

with the domain name gmx.com. The email referenced another real estate property and stated, "Hi Hillary, Could the sellers get their funds wired to their personal company account? I just got their request, please advise. Thanks."

18. On March 1, 2017, I received an email forwarded from Hillary Barbour that was from Google and had the subject "Delivery Status Notification (Delay)." The email stated that "There was a temporary problem delivering your message to gregthatcher46@gmail.com." Following receipt of this email, Barbour reviewed her Gmail account settings and discovered a setting that was forwarding a copy of incoming mail to the email addresses gregthatcher46@gmail.com and resultsnew1@gmail.com. Barbour had not created this setting and upon discovery removed it on March 2, 2017.

SUMMARY

19. As described above, the Gmail accounts listed in Attachment A were designated by unknown cyber actors to receive all email sent to Johnson & Finnigan LLP paralegal Hillary Barbour's work email account, hillary@jflawvt.com. Since Barbour's responsibilities included facilitating the closing of real estate transactions for clients of Johnson & Finnigan LLP, her email communications regularly contained details of these transactions including buyer and seller names, closing dates, and property addresses. Knowledge of this information would make it possible for cyber actors to develop targeted email schemes designed to defraud participants in the transaction from proceeds. A scheme of this type was used to defraud Johnson & Finnigan LLP of \$100,683.96 on September 16, 2016. As of February 2017, unknown cyber actors were continuing to target Johnson & Finnigan LLP with similar emails. Therefore, there is reason to believe the email accounts listed in Attachment A contain copies of email utilized to develop these attacks. There is

also reason to believe these email accounts contain information that could be utilized to identify the cyber actors controlling the accounts.

20. On November 1, 2016, the FBI provided a preservation letter to Google requesting that Google preserve any and all information associated with the email account gregthatcher46@gmail.com, pending further criminal process. On March 20, 2017, the FBI provided a letter to Google again requesting preservation of information associated with this account. On May 1, 2017, the FBI provided a preservation letter to Google requesting that Google preserve any and all information associated with the email account resultsnew1@gmail.com.

21. At this time, I am seeking a warrant requesting information associated with the email addresses listed in attachment A from the time of the creation of those accounts through the present. Based on the pattern of use of these accounts evident in this investigation, I believe the accounts contain information related to criminal activity. Based on my training and experience, I am aware that cyber criminals often will use email accounts for multiple criminal schemes as well as for personal matters, including shopping or social media interactions. During the course of these communications, cyber criminals often leave clues to their identities including other email addresses, information regarding physical location, names, or telephone numbers. Thus, even information outside the period of the immediate crime may provide valuable clues to the identity of the individuals behind the keyboard in the current offenses.

22. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google's servers

indefinitely. Even if the subscriber deletes the email, it may continue to be available on Googles's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

23. In my training and experience and based on my review of Google's website, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files. These materials may also be stored in association with a user's email address as part of "Google Drive," a service that allows users to store and share files online or "Google Docs," a service within "Google Drive" allowing collaborative work on

online documents by a number of different users. This feature can be particularly useful to users working from different locations.

25. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

26. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

27. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

28. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This

geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

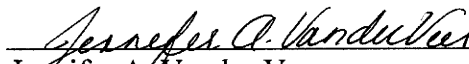
CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

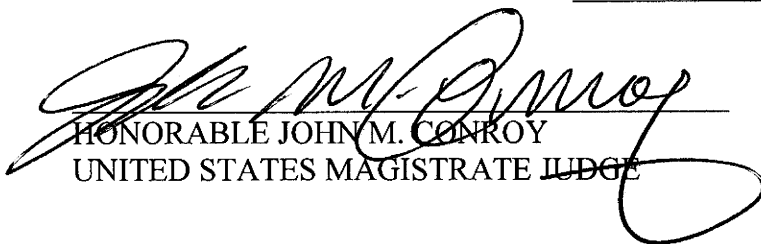
30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Jennifer A. Vander Veer
Special Agent
U.S. Federal Bureau of Investigation

Subscribed and sworn to before me on June 16, 2017



HONORABLE JOHN M. CONROY
UNITED STATES MAGISTRATE JUDGE